Hindawi Publishing Corporation
EURASIP Journal on Information Security
Volume 2010, Article ID 694797, 11 pages
doi:10.1155/2010/694797

Research Article

On the Implementation of Spread Spectrum Fingerprinting in Asymmetric Cryptographic Protocol

Minoru Kuribayashi (EURASIP Member)

Graduate School of Engineering, Kobe University, 1-1, Rokkodai, Nada, Kobe, Hyogo 657-8501, Japan

Correspondence should be addressed to Minoru Kuribayashi, kminoru@kobe-u.ac.jp

Received 14 October 2009; Accepted 28 January 2010

Academic Editor: Stefan Katzenbeisser

Digital fingerprinting of multimedia contents involves the generation of a fingerprint, the embedding operation, and the realization of traceability from redistributed contents. Considering a buyer's right, the asymmetric property in the transaction between a buyer and a seller must be achieved using a cryptographic protocol. In the conventional schemes, the implementation of a watermarking algorithm into the cryptographic protocol is not deeply discussed. In this paper, we propose the method for implementing the spread spectrum watermarking technique in the fingerprinting protocol based on the homomorphic encryption scheme. We first develop a rounding operation which converts real values into integer and its compensation, and then explore the tradeoff between the robustness and communication overhead. Experimental results show that our system can simulate Cox's spread spectrum watermarking method into asymmetric fingerprinting protocol.

1. Introduction

Due to the recent advances in broad-band network and multimedia technologies, the distribution and sharing of digital multimedia contents are increasing. It also helps a malicious party to duplicate and redistribute the contents, hence the protection of the ownership is strongly required. Encryption of the content cannot solve the problem because it must be ultimately decrypted at legitimate users who are the potential traitors in the future. Therefore, additional protection mechanisms are needed to discourage unauthorized redistribution. One of the mechanisms is the fingerprinting of multimedia which enables a seller to trace illegal users by embedding identification information into the content prior to distribution [1].

The research on fingerprinting techniques is classified into two studies: collusion resistant fingerprinting systems and cryptographic protocol. Since each user purchases a content containing his own fingerprint, each content is slightly different. If users collect some of them, they try to find the difference and delete/change the embedded information. In order to tolerate such an attack, designing collusion resistant fingerprint codes [2, 3] and orthogonal fingerprinting schemes like the spread spectrum watermarking technique [4] had been proposed. In a cryptographic protocol, the goal is to achieve the asymmetric property between a buyer and a seller such that only the buyer can obtain a uniquely watermarked content because of the threat of dispute. If both of the parties know the content, the buyer may redistribute a pirated copy but later repudiate it by insisting that the copy come from the seller.

In [5–9], the asymmetric protocol is performed by exploiting the homomorphic property of the public-key cryptosystem that enables a seller to obtain the ciphertext of watermarked content by operating an encrypted fingerprint with an encrypted content. Since the ciphertext is computed using a buyer's encryption key, only the buyer can decrypt it; hence, only he can obtain the watermarked content. It is also desirable for the fingerprinting protocol to solve the unbinding problem such that the relation between fingerprint information and a specific transaction performed by a buyer and a seller [10]. On the other hand, Pfitzmann and Sadeghi [5, 6] introduced the digital cash scheme to a fingerprinting protocol, and Camenisch [7] used

group signature schemes for the solution of the unbinding problem. In both schemes, bit commitment schemes are exploited at the embedding protocol using zero-knowledge proof because the protocol is performed only by a buyer and seller. For the realization of two-party protocol, their scheme sacrifices the selection of embedding information, namely a fingerprint. In their protocol, a fingerprint is a randomly selected integer by a buyer, and each bit of the fingerprint is committed to a seller for the security reason. In such a case, the encoding of the fingerprint by a collusion secure code [2, 3, 11] is difficult because the seller cannot check that the committed data is the codeword, and the exploitation of the spread spectrum watermarking technique is also difficult. In addition, the protocol of the zero-knowledge proof consumes much communicational resources for the transaction. These characteristics greatly degrade the practicality of the fingerprinting protocol.

The fingerprinting protocol in [10] introduced a trusted authority who generates a robust fingerprint when valid items of a certain transaction between a buyer and a seller are transmitted from the seller. Furthermore, the enciphering rate of the two-party protocol applied in the conventional schemes [6, 7] must be less than $1/10^3$ for the security of commitment schemes. If the data size of a content is 1 MB, the amount of communication data is more than 1 GB, which is extremely inefficient. In [9], the enciphering rate is drastically improved using a public-key cryptosystem with an additive homomorphism. Although the homomorphic property is effective for constructing asymmetric fingerprinting, there are still problems in its implementation.

In this paper, we propose the method for implementing the spread spectrum watermarking technique by carefully designing parameters for rounding operation. The preliminary version of this paper was presented in EUSIPCO2008 [12]. If frequency components of digital contents are used for the embedding of fingerprint information, they must be quantized in order to truncate real value to integer. Then, the precision of the frequency components should be considered in order not to degrade a watermarked image. When the spread spectrum watermarking technique in [4] is applied, the precision of the representing watermark signal is sensitive for the implementation. By scaling up the parameters by multiplying a constant factor, the precision is increased in our scheme. Then, the tradeoff between the scaling factor and the amount of data to be transmitted must be considered. In addition, for the characteristic of the fingerprinting protocol, frequency components and the watermark signal must be separately encrypted after quantization. In such a case, the consistency of the precision is a sensitive issue. Since an embedding operation is performed by addition of frequency components and a spread spectrum sequence, the additive homomorphic property of public-key cryptosystems [13, 14] can be directly exploited for the embedding. Then, the separate rounding operation causes interference terms in a deciphered data at a buyer side. Without loss of secrecy of an original content, the interference term is removed after decryption. The performance of our proposed method is evaluated by comparing it with the conventional scheme [4], which confirms the similar identification capability of illegal buyers.

2. Related Works

2.1. Asymmetric Property. If both a buyer and a seller obtain a watermarked content in a fingerprinting protocol, the seller cannot prove the illegal distribution by the buyer to a third party, even if the buyer's fingerprint is extracted. This is because the seller may distribute it himself in order to frame an innocent buyer. Hence, it is desirable that only a buyer is able to obtain his own fingerprinted content in the protocol. Such a protocol is called asymmetric fingerprinting protocol which concept was presented by Pfitzmann and Schunter [15]. In order to achieve such an asymmetric property, the homomorphic property of public-key cryptosystems is introduced in the fingerprinting protocols [8, 9, 16].

Let $E(M)$ be a ciphertext of a message M. The homomorphic property satisfies the following equation:

$$g(E(M_1), E(M_2)) = E\big(f(M_1, M_2)\big), \tag{1}$$

where $g(\cdot)$ and $f(\cdot)$ is one of the operations, *addition, multiplication, XOR,* and so forth, which is related to the applied cryptosystem and the embedding algorithm (Most public-key cryptosystems select multiplication for $g(\cdot)$). If M_1 is regarded as a digital content and M_2 as a fingerprint, the fingerprint can be embedded in the content without decryption by multiplying those ciphertexts. Since they are calculated using a buyer's public encryption-key, the watermarked content is decrypted only by the buyer, hence the asymmetric property is satisfied. The embedding operation based on the homomorphic property is basically performed for each element of fingerprint information which will be composed of bit-sequence or spread spectrum sequence, hence each element is separately embedded in its corresponding position. Thus, M_1 is not the entire content, but one of the components like the frequency elements to be fingerprinted by a watermarking technique. When the vector representation of M_1 is given by $\{m_{1,1}, m_{1,2}, m_{1,3}, \ldots\}$, the ciphertext is also represented as $E(M_1) = \{E(m_{1,1}), E(m_{1,2}), E(m_{1,3}), \ldots\}$. As a consequence, the detail of (1) is given by

$$g(E(m_{1,i}), E(m_{2,i})) = E(f(m_{1,i}, m_{2,i})), \quad (i = 1, 2, 3, \ldots). \tag{2}$$

Memon and Wong [8] apply multiplicative property of RSA scheme [17] to embed the fingerprint, and Pfitzmann and Sadeghi [5, 6] exploit bit commitment schemes based on the quadratic residues [18]. Kuribayashi and Tanaka [9] apply the additive homomorphic property of public-key cryptosystem such as Okamoto Uchiyama encryption scheme [13] and Paillier cryptosystem [14].

In watermarking techniques [1] for digital images, it is advisable to embed information in the frequency components for both the robustness and perceptual quality. However, as the frequency components are generally represented by real value, there is a difficult problem to apply cryptographic techniques directly because they are based on the algebraic property of integers. Many schemes [8, 10] ignored the implementation of watermarking algorithm into the asymmetric fingerprinting protocols, instead they

merely showed the validity of the cryptographic protocols which ensure the asymmetric property and the anonymity of buyers.

Considering the adaption of watermarking techniques for cryptographic fingerprinting protocol, a quantization method is useful as a fingerprint that can be embedded when the coefficients are quantized. In [9], the quantization index modulation based watermarking technique (QIM) [19] is applied for the embedding procedure because it rounds the values of frequency components in integers. Prins et al. [20] adapted three kinds of dithering modulations, which can improve the robustness of the QIM method, to the fingerprinting scheme, and implemented the method using a sufficiently large scaling factor. However, the enciphering rate is neglected. We assume that the bit-length of the message space is ℓ_M and that of each watermarked frequency components is ℓ_m. Generally, ℓ_M is much larger than ℓ_m. In order to exploit the message space effectively, dozens of watermarked frequency components are packed in one message in [9], hence, the enciphering rate is almost equivalent to that of an applied cryptosystem by suitably designing the message space of a ciphertext. It is remarkable that a negative number must be avoided because it is represented by much longer bit-sequence under the finite field of applied cryptosystem, which affects the other packed ones.

Although the capacity of embeddable information is large, considering the robustness against collusion attacks the spread spectrum watermarking technique is superior to QIM and its variants. In [8], the adaption of Cox's spread spectrum watermarking scheme [4] is discussed. Regretfully, there is a problem in the implementation because the rounding-off operation is not deeply considered for the spread spectrum watermarking algorithm.

2.2. Collusion Resilience. It is important to generate fingerprints that can identify colluders. In a fingerprinting scheme, each fingerprinted copy is slightly different, hence, malicious users will collect some copies with respective watermark in order to remove/alter the watermark. A number of works on designing fingerprints that are resistant against the collusion attack have been proposed. Many of them can be categorized into two approaches. One is to exploit the Spread Spectrum (SS) technique [4, 21, 22], and the other approach is to devise an exclusive code, known as collusion-secure code [2, 3, 11], which has traceability of colluders.

In the former approach, spread spectrum sequences which follow a normal distribution are assigned to users as fingerprints. The origin of the spread spectrum watermarking scheme is Cox's method [4] that embeds the sequence into frequency components of digital image and detects it using a correlator. Since normally distributed values allow the theoretical and statistical analysis of the method, modeling of a variety of attacks have been studied. Studies in [21] have shown that a number of nonlinear collusions such as interleaving attack can be well approximated by averaging collusion plus additive noise. So far, many variants of the spread spectrum watermarking scheme are based on the Cox's method.

Since the QIM watermarking technique [9] and its variants [20] are aiming at the extraction of a watermark bit-sequence, the latter approach is suitable to implement. The practicality of the latter approach is, however, restricted because of the long code length. In [23], the capability of QIM for the latter approach has been explored. The results show that one variant, which is called the spread transform dither modulation (STDM), retains an advantage under the blind detection. Under the non-blind detection, which is a reasonable assumption in a fingerprinting system, there is still a performance gap with the spread spectrum method. Moreover, in [24], the traceability is further improved by combining a spread spectrum embedding like Cox's method. Hereafter, we focus on the implementation of Cox's method in a fingerprinting protocol.

Let W be a watermark signal composed of L elements $w_i \in N(0,1)$, $(1 \le i \le L)$ and each of them is embedded into selected DCT coefficient $x_i, (1 \le i \le L)$ based on the following equation:

$$x_i' = x_i(1 + \alpha w_i), \tag{3}$$

where $N(0,1)$ is a normal distribution with mean 0 and variance 1, and α is an embedding strength. At the detector side, we determine which SS sequence is present in a test image by evaluating the similarity of sequences. From the suspicious copy, a sequence $\widetilde{W}$ is detected by calculating the difference from the original image, and its similarity with W is obtained as follows:

$$\mathrm{sim}\left(W, \widetilde{W}\right) = \frac{W \cdot \widetilde{W}}{\sqrt{\widetilde{W} \cdot \widetilde{W}}}. \tag{4}$$

If the value exceeds a threshold, the embedded sequence is regarded as W. When an original image is available, the above similarity measurement is valid because the main interference term, which is the frequency components of the original image, can be completely removed at the detection. However, under the blind detection, the removal of the interference term becomes a serious problem for an optimum detection. There are some related works [25, 26] concerning to the problem. Since our scope is to implement the spread spectrum method on the encrypted domain in the asymmetric protocol, the detail of the related works is omitted in this paper. Furthermore, in a fingerprinting, it is assumed that an original image is available at the detection because the operation is performed by the author or his agent. Hence, at the detection, DCT coefficients of a test image are subtracted from those of the original image, and then the correlations with every candidates of watermark signal are computed. Thus, non-blind and informed watermarking scheme can be applied.

A simple, yet effective collusion attack is to average some variants of copy because when c copies are averaged, the similarity value calculated by (4) results in shrinking by a factor of c, which will be roughly $\sqrt{L}/c$ [4]. Even in this case, we can detect the embedded watermark and identify colluders by using an appropriately designed threshold.

2.3. Unbinding Problem. In the elementary fingerprinting protocol [8] involving a trusted authority, fingerprint information to be embedded is not well considered, which is merely related to user's information such as name, address, phone number, e-mail address, and so forth. When a seller finds an illegal copy and detects the corresponding buyer by extracting the fingerprint, he will go to court with the collected proofs. A malicious seller, however, frames the detected buyer by embedding the obtained fingerprint into other contents which are more expensive than the detected one that he really sold to the buyer. Therefore, once a seller obtains a fingerprint, it is possible for him to transplant it into another more expensive contents so that he can get compensated more.

In [10], a fingerprint is binded with a common agreement (ARG) by producing the signature of a trusted watermark certification authority (WCA), and the transaction of digital contents is uniquely associated with a log file. For anonymity of buyers, a digital certification authority (CA) is introduced in the fingerprinting protocol. A buyer B first randomly selects a key pair $(pk_{\mathrm{B}}, sk_{\mathrm{B}})$, where pk_{B} and sk_{B} are the public and secret keys of public-key cryptosystem, respectively. He sends pk_{B}, which is a pseudonym associated with B, to CA in order to get an anonymous certificate $\mathrm{Cert}_{\mathrm{CA}}(pk_B)$. When B makes an order to a seller S, he checks the validity of $\mathrm{Cert}_{\mathrm{CA}}(pk_{\mathrm{B}})$. Then S asks WCA to generate a unique watermark W for the current transaction between B and S. The protocol between the buyer B and seller S is summarized below (the detail is referred to [10]).

(1) B selects one-time key pair (pk, sk) and generates its certificate $\mathrm{Cert}_{pk_{\mathrm{B}}}(pk)$ using the public key pk_{B}. After making a common agreement ARG, B calculates a digital signature $\mathrm{Sign}_{pk}(\mathrm{ARG})$ using the one-time public key pk. B sends pk_{B}, pk, $\mathrm{Cert}_{\mathrm{CA}}(pk_{\mathrm{B}})$, $\mathrm{Cert}_{pk_B}(pk)$, ARG, and $\mathrm{Sign}_{pk}(\mathrm{ARG})$ to S.

(2) If the validity of the received items is verified, S generates a watermark V and embeds it into contents X. The watermarked one is denoted by $X^{(V)}$. The watermark is reference information to retrieve this sale record from illegally distributed copy; hence it could be omitted if the seller wants to avoid the degradation of quality. Then, S send $\mathrm{Cert}_{pk_B}(pk)$, ARG, $\mathrm{Sign}_{pk}(\mathrm{ARG})$, and $X^{(V)}$ to WCA.

(3) Upon receiving the items, WCA verifies the validity of the certificate and signature, and reject the transaction if any of them is invalid. Otherwise, using $X^{(V)}$ it generates an unique and robust watermark W as fingerprint information which is specific to this transaction. Then, it computes $E_{pk}(W)$, $E_{pk_{\mathrm{WCA}}}(W)$, and $\mathrm{Sign}_{\mathrm{WCA}}(E_{pk}(W), pk, \mathrm{Sign}_{pk}(\mathrm{ARG}))$, and sends them back to S.

(4) When S receives the response, the embedding operation in encrypted domain is performed by computing

$$E_{pk}\left(X^{(W,V)}\right) = E_{pk}\left(X^{(V)}\right) \oplus E_{pk}(W), \tag{5}$$

where $\oplus$ implies the embedding operation based on the homomorphic property. Then, S delivers $E_{pk}(X^{(W,V)})$ to B.

(5) After decrypting the received $E_{pk}(X^{(W,V)})$, B obtains the watermarked content $X^{(W,V)}$,

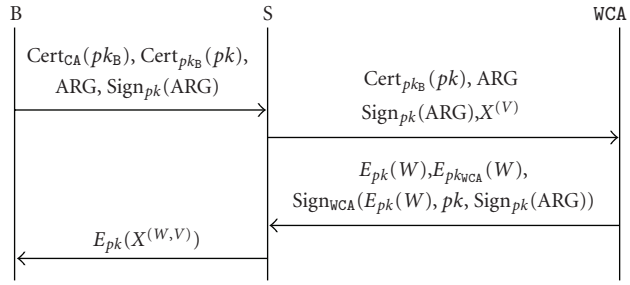


Figure 1: The transaction of the fingerprinting protocol.

where $E_{pk}(\cdot)$ is an enciphering function using a public key pk. The flow of the transaction is summarized in Figure 1.

3. Implementation for Watermarking Algorithm

In this section, we show how to implement the spread spectrum watermarking technique [4] in the fingerprinting protocol based on the homomorphic property of public-key cryptosystem. Hereafter, for simplicity, the embedding of the reference information V is omitted in the protocol, and we assume that an original image is composed of $M \times N$ pixels and is represented by the DCT selected coefficients x_i, $(1 \le i \le L)$ and the remaining ones x_i, $(L+1 \le i \le MN)$.

3.1. Embedding. The embedding operation in (3) can be easily performed using the additive homomorphic property of public-key cryptosystems such as the Okamoto-Uchiyama encryption scheme [13] and the Paillier cryptosystem [14]. Remember that (3) is composed of two operations; multiplication and addition for $g(\cdot)$ and $f(\cdot)$, respectively. Since the multiplication is realized by the iteration of addition, the embedding operation is represented by the multiplication and exponentiation as follows:

$$E_{pk}(x_i(1 + \alpha w_i)) = E_{pk}(x_i) \cdot E_{pk}(w_i)^{\alpha x_i}. \tag{6}$$

The above operation can be directly applied for the operation $\oplus$ in (5). Here, it is noticed that a watermark signal and DCT coefficients are generally represented by real values and they must be rounded to integers before the encryption. If such parameters are directly rounded to the nearest integers, it may result in the loss of information. Hence, they should be scaled before rounding-off. In addition, negative numbers should be avoided considering the property of a cryptosystem as mentioned in Section 2.1 Hence, a rounding operation that maps real value into positive integer is required.

At first, we show the operation concerning to a watermark signal $W = \{w_1, w_2, w_3, \ldots, w_L\}$. Since the ciphertext of W is computed by a watermark certification authority WCA, the enciphering operation is performed previously sent to a seller S. A constant positive integer value p_w is added to each element of watermark signal w_i, $(1 \le i \le L)$ to make the value positive. Then, it is scaled by a factor of s_w in order to keep the degree of precision, and it is quantized to $\overline{w}_i$. Such operations are formalized by the following one equation:

$$\begin{aligned}\overline{w}_i &= \mathrm{int}(s_w(w_i + p_w)) \\ &= s_w(w_i + p_w) + \epsilon_{w_i}, \quad 1 \le i \le L,\end{aligned} \tag{7}$$

where $\mathrm{int}(a)$ outputs the nearest integer from a real value a, and ϵ_{w_i} is the quantization error of $\overline{w}_i$. After the operation, WCA encrypts $\overline{W} = \{\overline{w}_1, \overline{w}_2, \overline{w}_3, \ldots, \overline{w}_L\}$ using a public key pk, and the ciphertexts $E_{pk}(\overline{W}) = \{E_{pk}(\overline{w}_1), E_{pk}(\overline{w}_2), E_{pk}(\overline{w}_3), \ldots, E_{pk}(\overline{w}_L)\}$, p_w and s_w are sent to S. It is noted that $E_{pk}(\overline{W})$ corresponds to $E_{pk}(W)$ in Figure 1, and the corresponding ciphertext of $E_{pk_{\mathrm{WCA}}}(\overline{W})$ is also sent to S.

Next, S performs the rounding operation to DCT coefficients x_i, $(1 \le i \le L)$ as follows. A positive integer value p_x is added to each DCT coefficient, and then scaled by $s_w s_x$. By quantizing it, the rounded DCT coefficient $\overline{x}_i$ is obtained:

$$\begin{aligned}\overline{x}_i &= \mathrm{int}(s_w s_x(x_i + p_x)) \\ &= s_w s_x(x_i + p_x) + \epsilon_{x_i}, \quad 1 \le i \le L,\end{aligned} \tag{8}$$

where ϵ_{x_i} is the quantization error of $\overline{x}_i$. For the control of rounding operation of each DCT coefficient, the watermark strength α is modified to $\overline{\alpha}_i$;

$$\begin{aligned}\overline{\alpha}_i &= \mathrm{int}(s_x \alpha |x_i|) \\ &= s_x \alpha |x_i| + \epsilon_{\alpha_i}, \quad 1 \le i \le L,\end{aligned} \tag{9}$$

where ϵ_{α_i} is the quantization error of $\overline{\alpha}_i$. Using the above items, S embeds $\overline{w}_i$ into $\overline{x}_i$ for $1 \le i \le L$ based on the additive homomorphic property of public cryptosystem as follows:

$$E_{pk}(\overline{x}_i) \cdot E_{pk}(\overline{w}_i)^{\overline{\alpha}_i} = E_{pk}(\overline{x}_i + \overline{\alpha}_i \overline{w}_i). \tag{10}$$

Since the plain value of the ciphertext $E_{pk}(\overline{x}_i + \overline{\alpha}_i \overline{w}_i)$ is

$$\begin{aligned}\overline{x}_i + \overline{\alpha}_i \overline{w}_i &= \mathrm{int}(s_w s_x(x_i + p_x)) \\ &\quad + \mathrm{int}(s_x \alpha |x_i| s_w(w_i + p_w)) \\ &= s_w s_x(x_i + \alpha w_i |x_i| + (p_x + \alpha |x_i| p_w)) \\ &\quad + s_x \alpha |x_i| \epsilon_{w_i} + s_w(w_i + p_w)\epsilon_{\alpha_i} + \epsilon_{x_i} + \epsilon_{\alpha_i}\epsilon_{w_i}.\end{aligned} \tag{11}$$

The scaling factor $s = s_w s_x$ and the adjustment factor $p = \mathrm{int}(p_x + \alpha |x_i| p_w)$ are necessary to calculate the actual watermarked DCT coefficients $x_i + \alpha w_i |x_i|$. The reason why p is rounded to an integer is explained in Section 3.4 Therefore, these two parameters s and p are sent to B as well as $E_{pk}(\overline{x}_i + \overline{\alpha}_i \overline{w}_i)$. It is noticed that the remaining DCT coefficients x_i, $(L + 1 \le i \le MN)$ should be sent to B. In order to keep the secrecy of the embedding position, they must be encrypted before delivery. Without loss of generality, the rounding operation for those coefficients are given by

$$\begin{aligned}\overline{x}_i &= \mathrm{int}(s_x s_w(x_i + p)) \\ &= s_x s_w(x_i + p) + \epsilon_{x_i}, \quad L + 1 \le i \le MN,\end{aligned} \tag{12}$$

and the ciphertexts $E_{pk}(\overline{x}_i)$ are sent with $E_{pk}(\overline{x}_i + \overline{\alpha}_i \overline{w}_i)$ to B. Namely, the ciphertexts of a watermarked image $E_{pk}(\overline{X^W})$, which is corresponding to $E_{pk}(X^{(W,V)})$ in Figure 1, is composed of those ones.

3.2. Decryption and Post-Processing. After the decryption of the received ciphertexts $E_{pk}(\overline{X^W})$, B divides the results by a factor of s, and then subtracts p as the post-processing operation. It is noticed that the adjustment factor p contains a rounding error ϵ_{p_i}, so it is rewritten by

$$p = p_x + \alpha |x_i| p_w + \epsilon_{p_i}. \tag{13}$$

At the embedding position, the ciphertexts are $E_{pk}(\overline{x}_i + \overline{\alpha}_i \overline{w}_i)$ and the post-processing operation outputs the watermarked coefficients $x_i + \alpha w_i |x_i|$ as follows:

$$\frac{D_{sk}\left(E_{pk}(\overline{x}_i + \overline{\alpha}_i \overline{w}_i)\right)}{s} - p = x_i + \alpha w_i |x_i| + \epsilon_i, \quad 1 \le i \le L, \tag{14}$$

where $D_{sk}(\cdot)$ is a deciphering function using a secret key sk and ϵ_i is the total rounding error represented by

$$\epsilon_i = \frac{\alpha |x_i| \epsilon_{w_i}}{s_w} + \frac{(w_i + p_w)\epsilon_{\alpha_i}}{s_x} + \frac{\epsilon_{x_i} + \epsilon_{\alpha_i}\epsilon_{w_i}}{s_x s_w} - \epsilon_{p_i}. \tag{15}$$

At the other position, the ciphertexts are $E_{pk}(\overline{x}_i)$ and B obtains x_i after the postprocessing operation:

$$\frac{D_{sk}\left(E_{pk}(\overline{x}_i)\right)}{s} - p = x_i + \frac{\epsilon_{x_i}}{s_x s_w}, \quad L + 1 \le i \le MN. \tag{16}$$

It is remarkable that the embedding position is kept secret from B, the classification of the above operations is difficult.

3.3. Amount of Quantization Error. If an original image is available at the detection, the embedded watermark signal is extracted by calculating the differences of pirated copy's DCT coefficients from the original ones. The extracted signal $\widetilde{w}_i$ must contain the quantization error caused by the rounding operation at embedding, and it is represented by

$$\begin{aligned}\widetilde{w}_i &= \frac{(x_i + \alpha w_i |x_i| + \epsilon_i) - x_i}{\alpha |x_i|} \\ &= w_i + \frac{\epsilon_i}{\alpha |x_i|}, \quad 1 \le i \le L.\end{aligned} \tag{17}$$

The amount of quantization error $\epsilon_i / \alpha |x_i|$ depends on the parameters s_w, s_x, p_w, and p_x:

$$\frac{\epsilon_i}{\alpha |x_i|} = \frac{\epsilon_{w_i}}{s_w} + \frac{(w_i + p_w)\epsilon_{\alpha_i}}{\alpha |x_i| s_x} + \frac{\epsilon_{x_i} + \epsilon_{\alpha_i}\epsilon_{w_i}}{\alpha |x_i| s_x s_w} - \frac{\epsilon_{p_i}}{\alpha |x_i|}. \tag{18}$$

It is noted that the values of the quantization errors ϵ_{w_i}, ϵ_{x_i}, ϵ_{α_i} and ϵ_{p_i} is uniformly distributed within the range $[-0.5, 0.5)$. So, if the scaling parameter s_w is small, the term ϵ_{w_i}/s_w remains as a dominant factor in $\epsilon_i/\alpha|x_i|$, and the quantization error is almost uniformly distributed in the range.

The energy of the quantization error in a watermarked copy is

$$\eta = \sum_{i=1}^{L} \left(\frac{\epsilon_i}{\alpha |x_i|} \right)^2. \tag{19}$$

Suppose that each watermarked copy contains a quantization error with energy η and c colluders average their copies. As the value of each copy's $\epsilon_i/\alpha|x_i|$ becomes $1/c$, the energy becomes η/c^2. The averaged copy contains the sum of such attenuated quantization error, hence the total energy of the quantization error in the averaged copy is estimated to be η/c. With the increase of c, the energy of the quantization error is to be dropped to $1/c$ of its original value.

3.4. Consideration. In Cox's method, a watermark W is selected from Gaussian distribution $N(0, 1)$. From the statistical property, when a parameter p_w is given, the error probability that $w_i + p_w$ is less than 0 is obtained as follows:

$$\Pr(w_i + p_w < 0) = \frac{1}{2} \operatorname{erfc}\left(\frac{p_w}{\sqrt{2}} \right), \tag{20}$$

where erfc() stands for the complementary error function. In other words, if the error probability is fixed, we can calculate the smallest integer p_w. For example, when $p_w = 5$, the error probability is $\Pr(w_i + p_w < 0) = 2.87 \times 10^{-7}$. Under a certain probability, when $w_i + p_w$ is less than 0, such a value is rounded to 0 in order to avoid the underflow. Considering the amount of the quantization error in (18), it is desirable to select p_w as small as possible.

In (3), the watermarked coefficient x_i' is composed of two terms; x_i and $\alpha w_i x_i$. Since w_i is encrypted at the center WCA prior to the embedding operation at S, x_i and w_i are rounded separately. Considering the post-processing at B, the scaling factors s_w, s_x, and the compensation factor p should be constant. Here, we assume that a constant value is uniformly added to real values which are w_i and x_i to make it positive. Then, B must subtract the interference term related to both x_i and w_i, which requires additional communication costs. If the adjustment factor p is varied with respect to x_i, the amount of information to be sent to B from S becomes very large. In order to avoid it, we set p a constant value by controlling the value p_x. Even if p and α is known and p_w is fixed, to obtain x_i is still informationally difficult because of two unknown parameters p_x and x_i for a given one equation $p = \operatorname{int}(p_x + \alpha|x_i|p_w)$. As a consequence, the secrecy of the original DCT coefficients is assured. If the value of p is sufficiently large, that of the parameter p_x is also large and hence the value of $x_i + p_x$ is positive.

3.5. Concatenation. Notice that if the values of scaling factors s_w are s_x are increased, the proposed scheme can simulate the original Cox method more precisely. From the viewpoint of enciphering rate, however, these factors should be small. Referring to [9], the bit-length of a watermarked coefficient $\overline{x}_i' = \overline{x}_i + \overline{\alpha}_i \overline{w}_i$, which is represented by a constant bit-length ℓ_x, is much smaller than that of message space in cryptosystems such as the Okamoto-Uchiyama encryption scheme [13] and the Paillier cryptosystem [14], and some of $\overline{x}_i'$ are packed in one message $\overline{M}$:

$$\overline{M} = \overline{x}_i' || \overline{x}_{i+1}' || \cdots || \overline{x}_{i+\delta-1}', \tag{21}$$

where $||$ denotes a concatenation and δ is the number of packed coefficients which is dependent on s_w and s_x. Such a packing operation is easily performed by computing the $2^{\ell_x t}$ th power of $E_{pk}(\overline{x}_{i+t}')$:

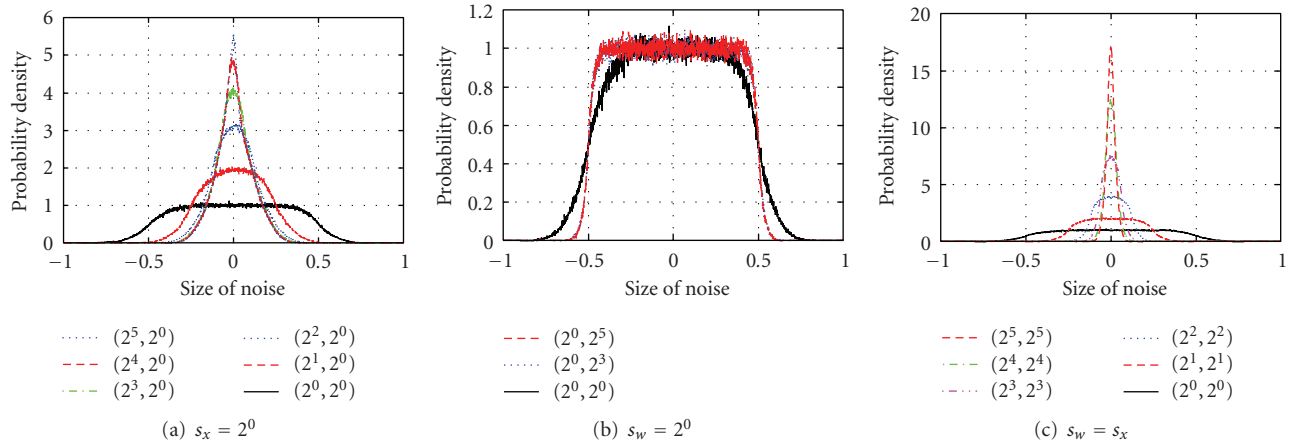
$$E_{pk}\left(\overline{M}\right) = \prod_{t=0}^{\delta-1} \left(E_{pk}\left(\overline{x}_{i+t}'\right) \right)^{2^{\ell_x t}}. \tag{22}$$

The appropriate size of s_w and s_x are explored by implementing them on a computer and evaluating the simulated performance. It is worth mentioning that the enciphering rate of the Paillier cryptosystem approaches asymptotically 1 using the extension of the cryptosystem [27] and then more data can be packed in one ciphertext. Although the works in [28, 29] can encode rational numbers by a limited precision, they are not suitable for the packing operation.

4. Experimental Results

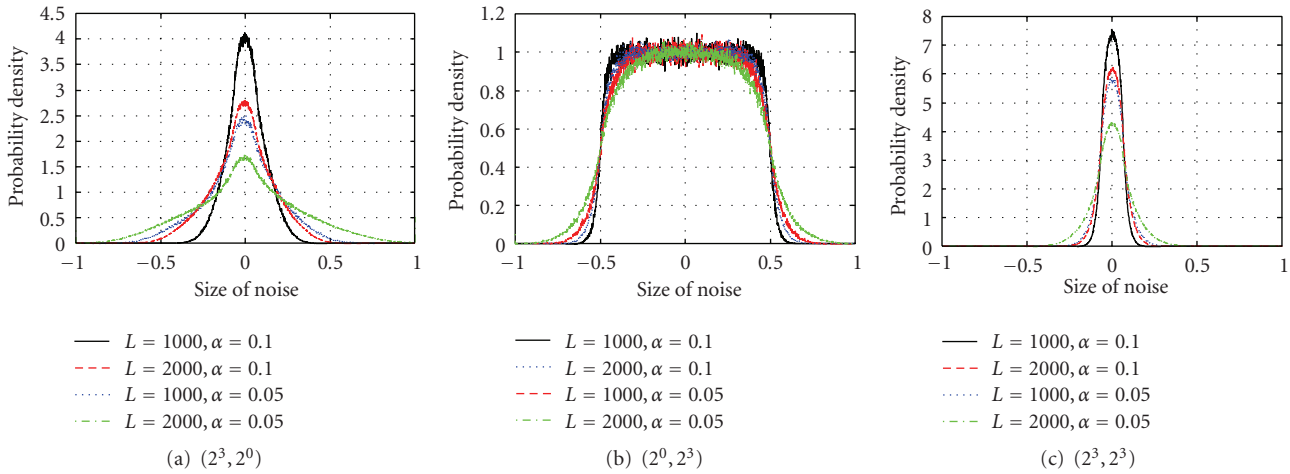
We have implemented our algorithm presented in Sect.3 and compared the performance with the original spread spectrum watermarking technique [4]. Since the basic algorithm of our scheme is Cox's scheme with a limited precision, we evaluate the degradation of an image by PSNR and the detected correlation values because it directly reflects the amount of changes between our fingerprinted image and the original fingerprinted one. If the results are similar, we regard that the performance of our simulated scheme is not degraded from that of the original one. In our simulation, a standard gray-scaled image "lenna" of 256×256 pixels is used, and the constant values are set $p_w = 5$ and $p = 10000$ (p_x is calculated by (13)). Even if p_w and p_x are added, the values of w_i and x_i might be negative. In such a case, the values are simply rounded to 0. In the following simulation, the number of simulation is 10^3 times, and the results are the averaged values.

A quantization error is caused by the rounding operation after orthogonal transformation which converts the frequency domain into the spatial domain as well as the rounding operation at the embedding of signal. For the evaluation of the quantization error $\epsilon_i/\alpha|x_i|$ shown in (18), the differences of watermarked images are calculated with respect to the scaling parameters s_w and s_x, and the probability density function (p.d.f.) is depicted in Figure 2 when $L = 1000$ and $\alpha = 0.1$ changing the scaling parameters



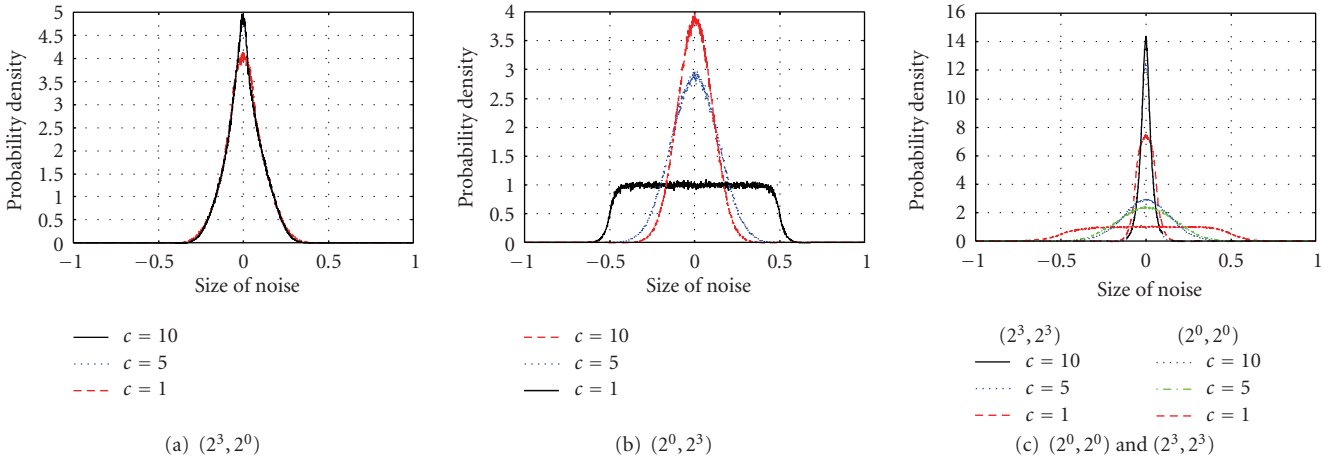
(a) $s_x = 2^0$ (b) $s_w = 2^0$ (c) $s_w = s_x$

FIGURE 2: The probability density function of the quantization error when $L = 1000$ and $\alpha = 0.1$, where the parenthetic numbers stands for the scaling parameters (s_w, s_x).



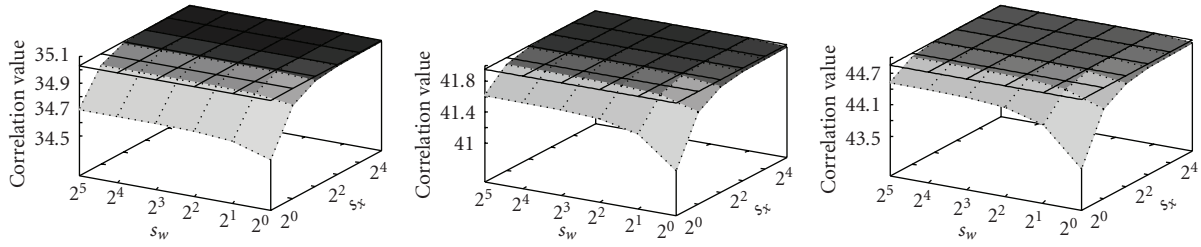
(a) $(2^3, 2^0)$ (b) $(2^0, 2^3)$ (c) $(2^3, 2^3)$

FIGURE 3: The probability density function of the quantization error for different L and α using the scaling parameters (s_w, s_x).



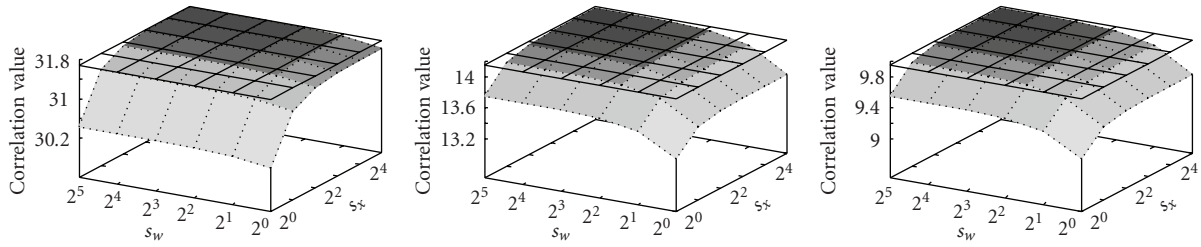
(a) $(2^3, 2^0)$ (b) $(2^0, 2^3)$ (c) $(2^0, 2^0)$ and $(2^3, 2^3)$

FIGURE 4: The probability density function of the quantization error under the averaging attack of c copies when $L = 1000$ and $\alpha = 0.1$ using the scaling parameters (s_w, s_x).



(a) $c = 1$ (b) $c = 5$ (c) $c = 10$

Figure 5: The image quality for the scaling values s_w and s_x when $L = 1000$ and $\alpha = 0.1$.



(a) $c = 1$ (b) $c = 5$ (c) $c = 10$

Figure 6: The average correlation value after averaging collusion attack for the scaling values s_w and s_x.

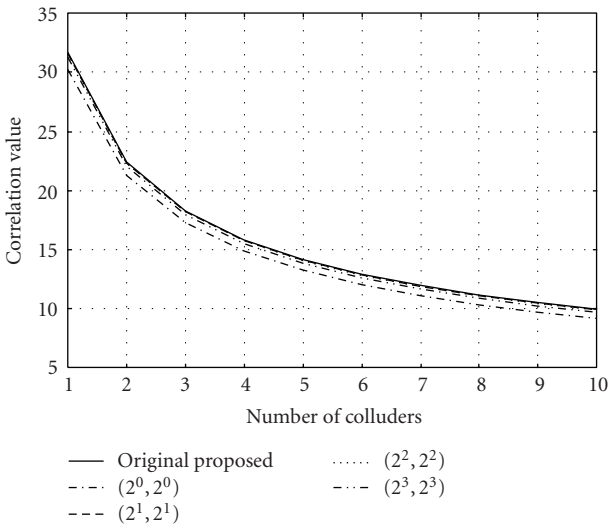


Figure 7: The average correlation value after averaging collusion attack for the number of colluders when $(s_w, s_w) = (2^3, 2^3)$.

s_w and s_x. Figure 2(a) shows the quantization error by fixing one scaling parameter $s_x = 2^0$. We can see that the shape of the p.d.f. is sharpened centering on zero with the increase of s_w. It is because of the decrease of the first term ϵ_{w_i}/s_w in (18). Figure 2(b) shows the quantization error by fixing the other scaling factor $s_w = 2^0$. It confirms that the value of the quantization error is almost uniformly distributed when s_w is small because the first term ϵ_{w_i}/s_w is not changed and it distributes uniformly in the range $[-0.5, 0.5]$. It is also noticed that the other terms in (18) is attenuated by the increase of s_x. Figure 2(c) confirms that the variance of

Table 1: The distribution of non-colluders' correlation values when $L = 1000$, $\alpha = 0.1$, and $(s_w, s_x) = (2^3, 2^3)$.

		mean	variance	max
No attack	original	−0.0107	0.9676	3.3252
	proposed	0.0020	0.9695	3.3030
Collusion	original	0.0182	0.9672	3.9882
($c = 5$)	proposed	0.0473	0.9649	3.8162
Collusion	original	0.0041	1.0075	4.0610
($c = 10$)	proposed	0.0045	1.0100	4.0568

the quantization error is decreased when both s_w and s_x are increased. Since the performance of Cox's scheme depends on the parameters L and α, the comparison of the p.d.f. is shown in Figure 3 using different values. We can see that the variance of the p.d.f. becomes large when L is increased and α is decreased. It is because the magnitude of selected DCT coefficients x_i becomes small when L is increased, hence, the value of the corresponding quantization error $\epsilon_i/\alpha|x_i|$ becomes large. It is remarked that the embedded signal energy as a watermark becomes smaller when α is decreased. In the following simulation, we use the parameters $L = 1000$ and $\alpha = 0.1$ for the evaluation.

It is important to evaluate the quantization error when a collusion attack is performed. Considering the studies in [21], we perform the averaging as the collusion attack. The changes in the quantization error are depicted in Figure 4 using several combination of s_w and s_x. We can see that there is a big changes of p.d.f. when $(s_w, s_w) = (2^0, 2^3)$ from Figure 4(b). It is because the first term ϵ_{w_i}/s_w in (18) follows Gaussian distribution considering the statistical property if c is sufficiently large.

Table 2: The degradation of the watermarked image when $(s_w, s_x) = (2^3, 2^3)$.

	aerial	baboon	barbala	f16	girl	lenna	peppers
Original	36.344	36.664	34.784	35.979	36.003	35.035	34.621
Proposed	36.338	36.659	34.779	35.974	35.997	35.030	34.615

Table 3: The degradation of the correlation values when $(s_w, s_x) = (2^3, 2^3)$.

		aerial	baboon	barbala	f16	girl	lenna	peppers
No attack	original	31.681	31.678	31.680	31.681	31.615	31.680	31.679
	proposed	31.657	31.645	31.651	31.653	31.579	31.650	31.650
Collusion	original	14.148	14.130	14.137	14.143	14.071	14.134	14.139
($c = 5$)	proposed	14.129	14.093	14.109	14.117	14.030	14.104	14.112
Collusion	original	9.989	9.946	9.960	9.975	9.863	9.954	9.966
($c = 10$)	proposed	9.969	9.901	9.928	9.946	9.813	9.920	9.935

For the comparison of the image quality, the degradation of watermarked images and averaged copies is shown in Figure 5. We can see that the PSNR of our method is approaching to the original one according to the increase of scaling parameters s_w and s_x, and the degradation of the PSNR is mainly dependent on s_x. It is because the first term ϵ_{w_i}/s_w in (18) becomes small with the increase of s_w. From the results, we can say that our watermarked images are very close to the original ones if $s_w \geq 2^2$ and $s_x \geq 2^3$.

For the evaluation of correlation values, we embed a watermark signal using the original Cox's scheme and our scheme. The comparison of correlation values for the watermark images is shown in Figure 6(a), where that of the original scheme is 31.680 depicted by black line on the top of the graph. The correlation values of averaged copies are also shown in Figures 6(b) and 6(c), where the original values are 14.134 and 9.954, respectively. We can see that the performance is asymptotically reaching the original value according to the increase of the scaling factors s_w and s_x. Different from the results of PSNR, the correlation values becomes very close to the original value if $s_w \geq 2^3$ and $s_x \geq 2^3$. This means that the quantization error degrades the correlation value much more than the value of PSNR. The results indicate that the correlation value is more sensitive to the noise injected to a watermarked image. The degradation of the correlation values is also compared by changing the number of colluders, which results are shown in Figure 7. From the results, we can say that the correlation values of our scheme using $s_w = s_w = 2^3$ are almost coincident with the original values.

The error (false-positive) probability is an important factor to evaluate the performance of fingerprinting scheme, and the probability is dependent on the design of the threshold for a correlation value to determine guilty. If our method uses the same design of the threshold as the original one, the changes of the probability can be evaluated by the distribution of non-colluders' correlation values. Using 10^4 watermark signals assigned for non-colluders, the correlation values are calculated. The mean and variance of the correlation values and the maximum values are shown Table 1. From the results, we can say that the distribution of our method is very similar to that of original one. It is remarkable that the maximum value of our method is slightly smaller than that of original one. This means that the error probability of our method is slightly improved.

From the above results, the degradation of performance from the original scheme is very slight, and it does not affect the robustness against attacks. It is noted that the scaling factors s_w and s_x is closely related to the degradation of performance. It is better to increase the value of these parameters, for example $s_w \geq 2^3$ and $s_x \geq 2^3$, but we have to consider the communication costs because the bit-length to represent the watermarked DCT coefficient $\overline{x}_i + \overline{\alpha}_i \overline{w}_i$ is increased according to the size of s_w and s_x, which degrades the coding rate of such information. For other images, "aerial", "baboon", "barbala", "f16", "girl", and "peppers", the similar results are derived with the above parameters as shown in Tables 2 and 3. The attenuation of PSNR value from the original one is at most 0.016%, that of the correlation value is at most 0.1%, and under the averaging collusion the attenuation is less than 0.39%. As a consequence, recommended parameters are $s_w = 2^3$ and $s_x = 2^3$ from our simulation results. It is expected that other kinds of spread spectrum watermarking schemes will be simulated with the similar precision, and the implementation is our future work.

When we use the above recommended parameters, the value of $\overline{x}'_i$ can be represented by 20 bits (the range must be within $[0, 2^{20}]$ if $s_w = s_x = 2^3$ and $p = 10000$). For the security reason, the bit-length of a composite $n = pq$ for the modulus of the Paillier cryptosystem should be no less than 1024 bits. When $|n| = 1024$, an 1024-bit message is encrypted to an 2048-bit ciphertext. Under the above condition, the number of watermarked DCT coefficients in one ciphertext is at most $\delta = 51 (= [1024/20])$. Since the number of DCT coefficients are $65536 = 256 \times 256$, the number of ciphertexts is 1286 ($= [65536/51]$) and the total size of the ciphertexts is about 2.5 MB, which is about 40 times larger than the original file size 66 KB. In the case that the packing is not performed, the total size is more than

128 MB. Therefore, the proposed method efficiently implements the Cox's spread spectrum watermarking scheme in the asymmetric fingerprinting protocol.

5. Conclusion

In this paper, we discuss about the implementation of the fingerprinting protocol based on the additive homomorphic property of public-key cryptosystems. The effects of rounding operation which maps a real value into a positive integer are formulated, and an auxiliary operation to obtain a watermarked content is presented. From our simulation results, the identification capability of our algorithm is quite similar to the Cox's algorithm, hence we can simulate the scheme on the cryptographic protocol with a limited precision.

Acknowledgment

This research was partially supported by the Ministry of Education, Culture, Sports Science and Technology, Grant-in-Aid for Young Scientists (B) (21760291), 2009.

References

[1] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Water-Marking*, Artech House, Boston, Mass, USA, 2000.

[2] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.

[3] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1069–1087, 2003.

[4] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[5] B. Pfitzmann and A. Sadeghi, "Coin-based anonymous fingerprinting," in *Proceedings of the Advances in Cryptology (EUROCRYPT '99)*, vol. 1592 of *Lecture Notes in Computer Science*, pp. 150–164, Springer, 1999.

[6] B. Pfitzmann and A. Sadeghi, "Anonymous fingerprinting with direct non-repudiation," in *Proceedings of the Advances in Cryptology (ASIACRYPT '00)*, vol. 1976 of *Lecture Notes in Computer Science*, pp. 401–414, Springer, 2000.

[7] J. Camenisch, "Efficient anonymous fingerprinting with group signatures," in *Proceedings of the Advances in Cryptology (ASIACRYPT '00)*, vol. 1976 of *Lecture Notes in Computer Science*, pp. 415–428, Springer, 2000.

[8] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 10, no. 4, pp. 643–649, 2001.

[9] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2129–2139, 2005.

[10] C.-L. Lei, P.-L. Yu, P.-L. Tsai, and M.-H. Chan, "An efficient and anonymous buyer-seller watermarking protocol," *IEEE Transactions on Image Processing*, vol. 13, no. 12, pp. 1618–1626, 2004.

[11] Y. Zhu, D. Feng, and W. Zou, "Collusion secure convolutional spread spectrum fingerprinting," in *Proceedings of the 4th International Workshop on Digital Watermarking (IWDW '05)*, vol. 3710 of *Lecture Notes in Computer Science*, pp. 67–83, Springer, 2005.

[12] M. Kuribayashi and M. Morii, "On the implementation of asymmetric fingerprinting protocol," in *Proceedings of the European Signal Processing Conference (EUSIPCO '08)*, 2008, SS7-1.

[13] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," in *Proceedings of the Advances in Crypgology (EUROCRYPT '98)*, vol. 1403 of *Lecture Notes in Computer Science*, pp. 308–318, Springer, 1998.

[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the Advances in Crypgology (EUROCRYPT '99)*, vol. 1592 of *Lecture Notes in Computer Science*, pp. 223–238, Springer, 1999.

[15] B. Pfitzmann and M. Schunter, "Asymmetric fingerprinting," in *Proceedings of the Advances in Crypgology (EUROCRYPT '96)*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 84–95, Springer, 1996.

[16] B. Pfitzmann and M. Waidner, "Anonymous fingerprinting," in *Proceedings of the Advances in Crypgology (EUROCRYPT '97)*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 88–102, Springer, 1997.

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[18] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *Journal of Computer and System Sciences*, vol. 37, no. 2, pp. 156–189, 1988.

[19] B. Chen and G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, 2001.

[20] J. P. Prins, Z. Erkin, and R. L. Lagendijk, "Anonymous fingerprinting with robust QIM watermarking techniques," *EURASIP Journal on Information Security*, vol. 2007, Article ID 31340, 13 pages, 2007.

[21] H. V. Zhao, M. Wu, Z. J. Wang, and K. J. R. Liu, "Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting," *IEEE Transactions on Image Processing*, vol. 14, no. 5, pp. 646–661, 2005.

[22] Z. J. Wang, M. Wu, H. V. Zhao, W. Trappe, and K. J. R. Liu, "Anti-collusion forensics of multimedia fingerprinting using orthogonal modulation," *IEEE Transactions on Image Processing*, vol. 14, no. 6, pp. 804–821, 2005.

[23] A. Swaminathan, S. He, and M. Wu, "Exploring QIM based anti-collusion fingerprinting for multimedia," in *Security, Steganography, and Watermarking of Multimedia Contents VIII*, vol. 6072, article 60721T of *Proceedings of SPIE*, San Jose, Calif, USA, 2006.

[24] Y. Yacobi, "Improved boneh-shaw content fingerprinting," in *Proceedings of Topics in Cryptology (CT-RSA '01)*, vol. 2020 of *Lecture Notes in Computer Science*, pp. 378–391, Springer, 2001.

[25] Q. Cheng and T. S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 906–924, 2003.

[26] M. Barni, F. Bartolini, A. de Rosa, and A. Piva, "Optimum decoding and detection of multiplicative watermarks," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1118–1123, 2003.

[27] I. Damgård and M. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in *Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC '01)*, vol. 1992 of *Lecture Notes in Computer Science*, pp. 119–136, Springer, 2001.

[28] P. A. Fouque, J. Stern, and G. J. Wackers, "Cryptocomputing with rationals," in *Proceedings of the Financial Cryptography*, vol. 2357 of *Lecture Notes in Computer Science*, pp. 136–146, Springer, 2003.

[29] C. Orlandi, A. Piva, and M. Barni, "Oblivious neural network computing via homomorphic encryption," *EURASIP Journal on Information Security*, vol. 2007, Article ID 37343, 11 pages, 2007.